Outline

- Protection mechanisms
  - Lead to …
- OS structures
- System and library calls
Protection Issues

- **CPU**
  - Kernel has the ability to take CPU away from users to prevent a user from using the CPU forever
  - Users should not have such an ability

- **Memory**
  - Prevent a user from accessing others’ data
  - Prevent users from modifying kernel code and data structures

- **I/O**
  - Prevent users from performing “illegal” I/Os

- **Question**
  - What’s the difference between protection and security?
Architecture Support: Privileged Mode

An interrupt or exception (INT)

User mode
- Regular instructions
- Access user memory

Kernel (privileged) mode
- Regular instructions
- Privileged instructions
- Access user memory
- Access kernel memory

A special instruction (IRET)
Privileged Instruction Examples

- Memory address mapping
- Flush or invalidate data cache
- Invalidate TLB entries
- Load and read system registers
- Change processor modes from kernel to user
- Change the voltage and frequency of processor
- Halt a processor
- Reset a processor
- Perform I/O operations
Monolithic

- All kernel routines are together, linked in single large executable
  - Each can call any other
  - Services and utilities
- A system call interface
- Examples:
  - Linux, BSD Unix, Windows, …
- Pros
  - Shared kernel space
  - Good performance
- Cons
  - Instability: crash in any procedure brings system down
  - Inflexible / hard to maintain, extend
Layered Structure

- Hiding information at each layer
- Layered dependency
- Examples
  - THE (6 layers)
    - Mostly for functionality splitting
  - MS-DOS (4 layers)
- Pros
  - Layered abstraction
- Cons
  - Inefficiency
  - Inflexible
x86 Protection Rings

- Operating system kernel
- Operating system services
- Applications

Privileged instructions can be executed only when the current privileged level (CPR) is 0.
Microkernel

- Services implemented as regular processes
- Micro-kernel obtain services for users by messaging with services
- Examples:
  - Mach, Taos, L4, OS-X
- Pros?
  - Flexibility
  - Fault isolation
- Cons?
  - Inefficient (boundary crossings)
  - Insufficient protection
  - Inconvenient to share data between kernel and services
  - Just shifts the problem?
Virtual Machine

- Virtual machine monitor
  - Virtualize hardware
  - Run several OSes
  - Examples
    - IBM VM/370
    - Java VM
    - VMWare, Xen

- What would you use virtual machine for?
Two Popular Ways to Implement VMM

VMM runs on hardware

VMM as an application

(A special lecture later in the semester)
System Call Mechanism

- **Assumptions**
  - User code can be arbitrary
  - User code cannot modify kernel memory

- **Design Issues**
  - User makes a system call with parameters
  - The call mechanism switches code to kernel mode
  - Execute system call
  - Return with results
Exceptions

- Sources
  - Hardware (by external devices)
  - Software: INT n

- Exceptions
  - Normal: faults, traps, aborts, and interrupts
  - Special software generated: INT 3
  - Machine-check exceptions

- See Intel document volume 3 for details
## Interrupt and Exceptions (1)

<table>
<thead>
<tr>
<th>Vector #</th>
<th>Mnemonic</th>
<th>Description</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>#DE</td>
<td>Divide error (by zero)</td>
<td>Fault</td>
</tr>
<tr>
<td>1</td>
<td>#DB</td>
<td>Debug</td>
<td>Fault/trap</td>
</tr>
<tr>
<td>2</td>
<td></td>
<td>NMI interrupt</td>
<td>Interrupt</td>
</tr>
<tr>
<td>3</td>
<td>#BP</td>
<td>Breakpoint</td>
<td>Trap</td>
</tr>
<tr>
<td>4</td>
<td>#OF</td>
<td>Overflow</td>
<td>Trap</td>
</tr>
<tr>
<td>5</td>
<td>#BR</td>
<td>BOUND range exceeded</td>
<td>Trap</td>
</tr>
<tr>
<td>6</td>
<td>#UD</td>
<td>Invalid opcode</td>
<td>Fault</td>
</tr>
<tr>
<td>7</td>
<td>#NM</td>
<td>Device not available</td>
<td>Fault</td>
</tr>
<tr>
<td>8</td>
<td>#DF</td>
<td>Double fault</td>
<td>Abort</td>
</tr>
<tr>
<td>9</td>
<td></td>
<td>Coprocessor segment overrun</td>
<td>Fault</td>
</tr>
<tr>
<td>10</td>
<td>#TS</td>
<td>Invalid TSS</td>
<td></td>
</tr>
</tbody>
</table>
## Interrupt and Exceptions (2)

<table>
<thead>
<tr>
<th>Vector #</th>
<th>Mnemonic</th>
<th>Description</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td>#NP</td>
<td>Segment not present</td>
<td>Fault</td>
</tr>
<tr>
<td>12</td>
<td>#SS</td>
<td>Stack-segment fault</td>
<td>Fault</td>
</tr>
<tr>
<td>13</td>
<td>#GP</td>
<td>General protection</td>
<td>Fault</td>
</tr>
<tr>
<td>14</td>
<td>#PF</td>
<td>Page fault</td>
<td>Fault</td>
</tr>
<tr>
<td>15</td>
<td>Reserved</td>
<td></td>
<td>Fault</td>
</tr>
<tr>
<td>16</td>
<td>#MF</td>
<td>Floating-point error (math fault)</td>
<td>Fault</td>
</tr>
<tr>
<td>17</td>
<td>#AC</td>
<td>Alignment check</td>
<td>Fault</td>
</tr>
<tr>
<td>18</td>
<td>#MC</td>
<td>Machine check</td>
<td>Abort</td>
</tr>
<tr>
<td>19-31</td>
<td>Reserved</td>
<td></td>
<td></td>
</tr>
<tr>
<td>32-255</td>
<td>User defined</td>
<td></td>
<td>Interrupt</td>
</tr>
</tbody>
</table>
System Calls

- Operating system API
  - Interface between an application and the operating system kernel

- Categories
  - Process management
  - Memory management
  - File management
  - Device management
  - Communication
How many system calls?

- 6th Edition Unix: ~45
- POSIX: ~130
- FreeBSD: ~130
- Linux: ~250 ("fewer than most")
- Windows 7: ?
V6/usr/sys/ken/sysent.c

/*
 * This table is the switch used to transfer
 * to the appropriate routine for processing a system call.
 * Each row contains the number of arguments expected
 * and a pointer to the routine.
 */

#include <sys/stat.h>

int sysent[] = {
    0, &nullsys, /* 0 = indir */
    0, &exit,   /* 1 = exit */
    0, &fork,   /* 2 = fork */
    2, &read,   /* 3 = read */
    2, &write,  /* 4 = write */
    2, &open,   /* 5 = open */
    0, &close,  /* 6 = close */
    0, &wait,   /* 7 = wait */
    2, &creat,  /* 8 = creat */
    2, &link,   /* 9 = link */
    1, &unlink, /* 10 = unlink */
    2, &exec,   /* 11 = exec */
    1, &chdir,  /* 12 = chdir */
    0, &time,   /* 13 = time */
    3, &mknod,  /* 14 = mknod */
    2, &chmod,  /* 15 = chmod */
    2, &chown,  /* 16 = chown */
    1, &break,  /* 17 = break */
    2, &stat,   /* 18 = stat */
    2, &seek,   /* 19 = seek */
    0, &getpid, /* 20 = getpid */
    0, &setuid, /* 21 = mount */
    0, &umount, /* 22 = umount */
    0, &setgid, /* 23 = setuid */
    0, &getuid, /* 24 = getuid */
    0, &stime, /* 25 = stime */
    3, &ptrace, /* 26 = ptrace */
    0, &fstat,  /* 27 = x */
    0, &lstat,  /* 28 = lstat */
    0, &stat,  /* 29 = x */
    1, &nullsys, /* 30 = smdate; inoperative */
    1, &tty,    /* 31 = stty */
    1, &gtty,   /* 32 = gtty */
    0, &nosys,  /* 33 = x */
    0, &nice,   /* 34 = nice */
    0, &sync,   /* 35 = sync */
    1, &kill,   /* 36 = kill */
    0, &swait,  /* 37 = swait */
    0, &sync,   /* 38 = sync */
    0, &lstat,  /* 39 = x */
    0, &nosys,  /* 40 = x */
    0, &nosys,  /* 41 = dup */
    0, &pipe,   /* 42 = pipe */
    1, &times,  /* 43 = times */
    4, &profil, /* 44 = prof */
    0, &nosys,  /* 45 = tiu */
    0, &setgid, /* 46 = setgid */
    0, &getgid, /* 47 = getgid */
    0, &getpid, /* 48 = sig */
};
OS Kernel: Trap Handler

- HW Device Interrupt
- System Call
- HW exceptions
- SW exceptions Virtual address exceptions

HW implementation of the boundary

- Syscall table
- System Service dispatcher
- Interrupt service routines
- System services
- Exception dispatcher
- VM manager’s pager
- Exception handlers
Passing Parameters

- **Pass by registers**
  - # of registers
  - # of usable registers
  - # of parameters in system call
  - Spill/fill code in compiler

- **Pass by a memory vector (list)**
  - Single register for starting address
  - Vector in user’s memory

- **Pass by stack**
  - Similar to the memory vector
  - Procedure call convention
Example:

```c
int read( int fd, char * buf, int size)
{
    move fd, buf, size to R1, R2, R3
    move READ to R0
    int $0x80
    move result to R_result
}
```

Linux: 80
NT: 2E
System Call Entry Point

**EntryPoint:**
- switch to kernel stack
- save context
- check $R_0$
- call the real code pointed by $R_0$
- place result in $R_{result}$
- restore context
- switch to user stack
- iret (change to user mode and return)

(Assume passing parameters in registers)
Design Issues

- **System calls**
  - There is one result register; what about more results?
  - How do we pass errors back to the caller?
  - Can user code lie?

- **System calls vs. library calls**
  - What should be system calls?
  - What should be library calls?
Backwards compatibility...

NAME

open - open a file

SYNOPSIS

```c
#include <sys/stat.h>
```

```c
#include <fcntl.h>
```

```c
int open(const char *path, int oflag, ...);
```

The use of `open()` to create a regular file is preferable to the use of `creat()`, because the latter is redundant and included only for historical reasons.
Division of Labor (or Separation Of Concerns)

Memory management example

- **Kernel**
  - Allocates “pages” with hardware protection
  - Allocates a big chunk (many pages) to library
  - Does not care about small allocs

- **Library**
  - Provides malloc/free for allocation and deallocation
  - Application use these calls to manage memory at fine granularity
  - When reaching the end, library asks the kernel for more
Summary

- Protection mechanism
  - Architecture support: two modes
  - Software traps (exceptions)
- OS structures
  - Monolithic, layered, microkernel and virtual machine
- System calls
  - Implementation
  - Design issues
  - Tradeoffs with library calls